UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

IN RE GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	Case No. 12-MD-2358 (SLR)
This Document Relates to: **All Actions**	

PLAINTIFFS' BRIEF IN OPPOSITION TO DEFENDANTS MEDIA INNOVATION GROUP, LLC AND WPP PLC'S MOTION TO DISMISS

KEEFE BARTELS, LLC
Stephen G. Grygiel (Del Br No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefbartels.com

Executive Committee Member

STRANGE & CARPENTER
Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.
James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertston, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

FINGER & SLANINA, LLC
Charles Slanina (DE Bar ID #2011)
David L. Finger (DE Bar ID #2556)
One Commerce Center
1201 N. Orange St., 7th fl.
Wilmington, DE 19801
(302) 573-2525
dfinger@delawgroup.com

Liaison Counsel

Additional Counsel on Signature Page

Dated: May 29, 2013

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

RULES

I. NATURE AND STAGE OF THE PROCEEDINGS

Plaintiffs filed their Consolidated Amended Complaint ("CAC") in this MDL on December 19, 2012. Defendants Media Innovation Group, LLC ("Media") and WPP PLC ("WPP," and with Media, "Defendants") filed a Motion to Dismiss under Fed. R. Civ. P. 12(b)(6) ("D. Br."). Plaintiffs' opposition follows.

II. SUMMARY OF ARGUMENT

1. Long on adjectives and assurances based on other cases that Plaintiffs' CAC is much ado about "harmless cookies" (D Br. 1), Defendants' Motion to Dismiss ignores Plaintiffs' factual allegations of Defendants' knowing misuse of cookies and the well-pled facts and anti-dismissal inferences of *this* CAC by *these* Plaintiffs. *See* CAC ¶¶ 153-160 (Media), ¶¶ 161-162 (WPP). These facts properly allege Plaintiffs' Wiretap, Stored Communications, and Computer Fraud and Abuse Act claims.

2. Defendants neglect what this Court has stated is proper Rule 12(b)(6) analysis: "accept all factual allegations in a complaint as true and take them in the light most favorable to plaintiff." *In re Wilmington Trust ERISA Litig*., Civ. No. 10–1114–SLR, 2013 WL 1855756, at *6 (D. Del. May 3, 2013) (citing *Erickson v. Pardus*, 551 U.S. 89, 94 (2007) and *Christopher v Harbury*¸ 536 U.S. 403, 406 (2002)) (Robinson, J.). Citing *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 545 (2007) for application of Fed. R. Civ. P. 8(a)'s governing "'short and plain statement of the claim'" test (*Wilmington Trust*, at *6), this Court has already rejected Defendants' effort to impose a more stringent pleadings test than Rule 8(a)(2)'s. *Id*. Defendants ignore the liability inferences to which Plaintiffs are entitled from the CAC's facts. *See McTernan v. City of York*, 577 F. 3d 521, 526 (3d Cir. 2009).

3. Defendants say "the CAC's allegations establish only that the Moving Defendants interacted with Plaintiffs' Safari browsers precisely as those browsers were designed to function,

and that *Plaintiffs themselves* initiated these harmless interactions. D. Br. 1 (emphasis in original). But the CAC factually alleges the Defendants deliberately tricked the browsers through a sophisticated ruse permitting the otherwise blocked setting of Media's "ZAP ID cookie," and WPP's OAX cookie. *See* CAC ¶¶ 153-54, 156, 161. Claiming Plaintiffs neither suffered any harm nor were "otherwise *affected in any way*" by Defendants' secret tracking (D. Br. 1, emphasis in original) Defendants wish away the CAC's allegations of illicit PII collection.

III. STATEMENT OF FACTS

Plaintiffs' factual allegations are deemed true on this motion. *See Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008). Misrepresenting and ignoring the CAC's facts, Defendants say "according to Plaintiffs' allegations, internet users see ads based on an intentional interaction between the user's browser (which initiates this interaction) and the third-party ad-serving company." D. Br. 2. Defendants ignore the key fact, deemed true here and which Defendants never denied (*see* CAC ¶¶ 159, 160 (Media); 162 (WPP)), that Defendants surreptitiously hacked the Safari browser's default third-party-cookie-blocking setting:

> As it sent its clients' advertisements to webpages requested by users making GET requests, Media included secret code, or, what Mr. Mayer described as "a script," in certain Media advertising. That secret script tricked the user's browser into sending an invisible form to Media, in turn deactivating Safari's privacy protection. Media then implanted an "id" cookie on the unknowing user's browser. CAC ¶ 153.[1]

Defendants are internet advertising companies dependent on compiling user-specific information permitting carefully targeted advertising. *See, e.g.*, CAC ¶¶ 25, 26, 161. Defendants silently disabled the Safari browser's default setting to permit Defendants to set the "id" (CAC ¶¶ 153, 154, 156) and "OAX" (CAC ¶¶ 154, 161) cookies vital to Defendants' business of

[1] *See also* CAC ¶¶ 154, 161 (describing how WPP did the same).

gathering user data to facilitate serving targeted ads based on user preferences. CAC ¶¶ 156, 157, 161. Good grounds support the conclusion that Defendants acted intentionally. CAC ¶ 155.

Defendants' argument that cookies are "benign" (D. Br. 2, n.2) ignores that the Defendants intentionally and wrongly hacked Plaintiffs' computers (*see* CAC ¶¶ 153-155 (Media), 161-162 (WPP)) to permit the installation of third-party cookies that the Plaintiffs neither wanted nor knew about, and which their browsers were set up to *block.* While confirming Plaintiffs' claims that cookies permit correlation of PII with users (*see, e.g.*, CAC ¶¶ 39(b)(ii), 45, 46, 48, 78, 90, 95-98, 113, 121,147, 153, 154, 156, 158, 161), Defendants' claim that cookies merely permitted ad-serving companies like Defendants to associate cookie values with browser-generated information (D. Br. 3) similarly ignores the CAC's central point: that Defendants violated three federal statutes by tricking the Plaintiffs' browsers into accepting those cookies in the first place, in turn allowing Defendants to obtain personal information about Plaintiffs without their consent.

Defendants' "harmless cookies" claims ignore the important distinction between first-party cookies (*see* CAC ¶ 39(b)(i)) and the third-party tracking cookies Plaintiffs' browsers were set to block, and are used by ad-serving companies, such as Defendants, to track user behavior to increase their own revenues by selling more targeted advertising. *Id.* ¶¶ 39(b)(ii), 40-48. Defendants' "ordinary course of business" argument based on the "Partial-Allowance Setting" ignores Defendants' secret and illegal tricking of the Plaintiffs' browsers into permitting third-party cookies, facilitating the obtaining and tracking of PII. Defendants fail to address Plaintiffs' core allegation that Plaintiffs and other users ***did not*** submit a form. Rather, Defendants added code to *trick* the browser into believing the user had done so to trigger the exception to cookie blocking. CAC ¶¶ 77-78. Despite Defendants' best efforts to depict their trickery as innocent

and "benign," their activities allowed them to track user activity across websites and receive information Plaintiffs attempted to prevent them from receiving.

IV. LEGAL ARGUMENTS

A. COUNT I – THE COMPLAINT STATES A CLAIM UNDER THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")

"The paramount objective of the Wiretap Act is to protect effectively the privacy of communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). The 1986 ECPA Amendments extended this protection to data and electronic transmissions. *Id.*[2]

The CAC factually alleges: (1) Defendants were not parties to the communications they intercepted; otherwise they would not have needed to trick Plaintiffs' browsers; and, (2) Media and WPP "intercepted" the "contents" of communications between Plaintiffs and first-party websites by designing code that disabled Plaintiffs' browsers' "do not track settings".[3]

1. Defendants Were Not Parties to the Communications

Defendants invoke the Wiretap Act exception (18 U.S.C. § 2511(2)(d)) protecting a communication's intended recipient. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012). But Defendants were *not* intended parties to Plaintiffs' communications with first-party websites. Plaintiffs' browsers were set to ***prohibit*** Defendants from becoming so. CAC ¶¶ 69-73, 199. Illicit eavesdroppers, not "parties," Defendants accessed Plaintiffs' communications by tricking Plaintiffs' browsers into sending contents of their online communications with first-party websites to Defendants. CAC ¶¶ 153-162, 201-203. Defendants

[2] "…[L]egislation which protects electronic communications from interceptions…should be comprehensive, and *not limited to particular types or techniques of communicating*…. [W]hat is being protected is *the sanctity and privacy of the communication*." 132 Cong. Rec. H4039-01 (1986) 1986 WL 776505 (comments from Representative Kastenmeier) (emphasis added).

[3] Defendants here correctly eschew the weak Wiretap Act arguments of other defendants, including that Plaintiffs consented to interceptions and no intercepting "devices" were used.

baselessly argue their undisclosed codes, iframes, forms and cookies alchemize into an exception to Wiretap Act liability because those deceptions let Defendants in on Plaintiffs' communications. *See, e.g., In re iPhone Application Litig.,* 844 F. Supp. 2d at 1062. (where plaintiffs had not intended any communication, a Wiretap Act defendant "cannot manufacture a statutory exception through its own accused conduct").

Defendants' reliance on *In re DoubleClick, Inc. Privacy Litig.* is misplaced. *See* 154 F. Supp. 2d 497 (S.D.N.Y. 2001). *In re DoubleClick* did not involve the intentional circumvention of privacy settings:

> DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick's tracking. As plaintiffs' counsel demonstrated at oral argument, users can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways:…(2) ***configuring their browsers to block any cookies from being deposited.***

Id. at 504-05 (emphasis added). Our Plaintiffs' browsers had been configured to do just that. But Defendants used embedded code intentionally designed to bypass those settings.[4, 5]

[4] Defendants' reliance on the unpublished decision of *Yunker v. Pandora Media, Inc.* is equally misplaced. *See* No. 11–CV–03113 JSW, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013). There the court dismissed a Wiretap Act claim with leave to amend on allegations that a communication's intended recipient divulged that communication to third parties. *Id.* at *8. Our CAC alleges that Defendants were *not* intended parties to communications between Plaintiffs and first-party websites, and that Plaintiffs' web browsers *were specifically configured to prohibit the Defendants from accessing those communications*.

[5] Defendants' footnote suggestion that they had consent from websites the Plaintiffs visited is an affirmative defense they must establish. 18 U.S.C. § 2511(2)(d). *See In re Pharmatrak,* 329 F.3d at 19. It is not appropriately the subject of this motion. *Scott v. Kuhlman,* 746 F.2d 1377, 1378 (9th Cir. 1984) (citing Wright & Miller, *Federal Practice and Procedure,* § 1277 at 328-30 (affirmative defenses not proper on motion to dismiss unless no disputed issues of fact). Besides, consent "should not be casually inferred." *In re Pharmatrak*, 329 F.3d at 20 (citation omitted). The CAC shows Defendants exceeded any consent they had to place an ad. Neither Plaintiffs nor the websites they visited consented to the tricking of Plaintiffs' browsers into accepting tracking technologies the browser was configured to block. CAC ¶¶ 201, 210. Numerous websites "were not aware of this behavior" and "would never condone it." CAC ¶ 126.

2. Media and WPP "Intercepted"[6] the "Content" of Communications

"Contents" under the Wiretap Act means "information concerning the substance, purport, or meaning of" a communication. 18 U.S.C. §2510(8). Seeking the shelter of inapplicable precedent saying "transactional data is not 'contents,'" Defendants impermissibly remodel the CAC's facts. Defendants intercepted transactional information *and* "contents."

Among other things, Defendants intercepted: (1) websites users visited; (2) what users viewed on those websites; (3) information users exchanged with websites; (4) information users had exchanged with the immediately preceding visited sites; (5) specific URLs Plaintiffs requested from first-party websites, which identified "specific items, such as websites, videos, pictures, or articles" that each Plaintiff chose to view; and (6) "information that Class Members exchanged with first-party websites during the course of filling out forms or conducting searches." CAC ¶¶ 205-207. Defendants intercepted "not just the fact of a request, but the exact request itself, which, because it includes URL information, is substantive." CAC ¶ 207.

Intercepting URLs is intercepting "content." *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (URL constitutes "content" because URL "identifies the particular document within a website that a person views and reveals much more information about the person's Internet activity"); *In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and Trap on [xxx]Internet Service Account/User Name*

[6] Plaintiffs have pled an "interception." CAC ¶¶ 153-162, 201-203. *See also United States v. Szymuskiewicz*, 622 F.3d 701, 707 (7th Cir. 2010); *In re Pharmatrak*, 329 F.3d at 21-22; *In re DoubleClick*, 154 F. Supp.2d at 514 (DoubleClick conceded its conduct violated 18 U.S.C. § 2511(1)(a)). 18 U.S.C. § 2510(4) defines "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device." The CAC details Defendants' use of computers and web servers to secretly embed code that fooled Plaintiffs' web browsers into sending Plaintiffs' communications with first-party websites to Defendants, allowing Defendants to acquire the contents of Plaintiffs' electronic communications. CAC ¶¶ 153-162, 201-203. Web servers and computers are devices by which an interception can occur. *See Szymusziewicz*, 622 F.3d at 707; *In re Pharmatrak*, 329 F.3d at 18-19.

[xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (URL constitutes "content" because "substance" and "meaning" of communication is user's search for information on particular topic).[7] Even the *Pen Register* case upon which Defendants rely recognizes the distinction between online transactional data (such as an IP address) and contents (such as a URL). *See In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and Trap & Trace Device on E-Mail Account,* 416 F. Supp. 2d 13, 17-18 (D.D.C. 2006) (pen register should "exclude all information relating to the subject line and body" of an email communication to avoid becoming "electronic intercepting device").

The same analysis applies to URLs. For instance, the URL http://articles.washingtonpost.com/2012-07-20/national/35488326_1_hiv-treatment-diane-havlir-infection is effectively the "subject line" of the communication between a user and a first-party website. By simply reading the URL, one discovers the user is requesting information about HIV treatments and infection. By following the link, one can see the full content of the communication. The URL gives the reader the "substance, purport, [and] meaning" of the communication. Defendants ignore the well principled distinction separating a URL from a phone number. D. Br. 8. URLs are "content."[8]

Finally, Defendants erroneously claim that the only additional information they gained from their secret codes was the alphanumeric value of the cookies that the code permitted Defendants to set. Not only are Plaintiffs entitled to discovery on that factual argument, but the

[7] For example, "[a] GET request for www.helpfordrunks.com with further information about where to find AA meetings in Wilmington," tells anyone intercepting such communication a great deal about the user. CAC ¶ 207.

[8] Also instructive, in *Brown v. Waddell,* 50 F.3d 285 (4th Cir. 1995), police obtained "pager clones" that intercepted additional number codes. One such code indicated that a caller was "en route." *Id*. at 287-88. The Fourth Circuit held that these additional numbers were "contents" under the Wiretap Act. *Id*. at 294. If numbers on a pager are "content," so too are the actual words and numbers in a URL string.

CAC shows that Defendants intercepted URL strings and information contained in online forms. Tricking the Plaintiffs' browser settings, Media placed its ZAP ID cookie, which collects and stores over 13 months of historical user-level data. CAC ¶ 154. Media also set WPP's OAX cookie. *Id*. These allegations show Defendants got much more from their cookies than numbers. Under all reasonable inferences, Defendants would not secretly have employed its multi-step bypassing of privacy settings to implant them. Defendants' cookies allowed Defendants to associate vast amounts of communications content (e.g. URL strings they have collected) with specific identifiable but unknowing users. CAC ¶¶ 205, 209.

B. COUNT II – THE COMPLAINT STATES A CLAIM UNDER THE STORED COMMUNICATIONS ACT

"[T]he Stored Communications Act protects individuals' privacy and proprietary interests." *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004). It provides a cause of action against "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system. . . ." 18 U.S.C. § 2701(a). The "'sort of trespasses to which the [ECPA] applies are those in which the trespasser gains access to information . . . which he is not entitled to see.'" *Therapeutic Research Faculty v. NBTY, Inc.*, 488 F. Supp. 2d 991, 997 (E.D. Cal. 2007) (quoting *Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, 497 (D. Md.2005)).

1. Defendants' Access Was in No Way Authorized

Defendants first argue that their "access" was not "without authorization." D. Br. 9. Defendants' assertion that its cookies were set in a manner specifically permitted by the Safari browser ignores the key fact that Defendants could only set those cookies by *tricking* Plaintiffs'

browsers, which were set to block those cookies. CAC ¶¶ 68-78, 153-156, 161, 217. To claim this illicit cookie-setting was "authorized" distorts "authorization" beyond any legitimate definition, including the interpretation Defendants cite in their footnote 6.

Defendants' reliance on *In re DoubleClick*, 154 F. Supp. 2d 497 is, again, misplaced. Defendants' surreptitious bypassing of the browser configurations, which *DoubleClick* suggested could block the collection of information (*id.* at 504-05[9]), defeats Defendants' *ipse dixit* (we did it, so it was authorized) authorization claim. Plaintiffs allege, and Defendants can show, no "conduct authorized" under 18 U.S.C. § 2701(c).

2. Browser-Managed Files on Computers and Mobile Devices are "Facilities" Through Which an ECS is Provided Under the SCA

Media and WPP argue, like their co-defendant Vibrant, that the CAC fails to allege that Media and WPP accessed a "facility" through which "electronic communications services" ("ECS") are provided. In their response to Vibrant's motion to dismiss, Plaintiffs show why this argument fails. That response is equally applicable to Defendants and is incorporated herein.

3. Defendants were Not Legally Authorized to Receive Information from the Illicitly-Set Third-Party Cookies

Defendants' arguments cannot remodel Plaintiffs' case's facts to resemble those in *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263 (N.D. Cal. 2001). In *Crowley*, Amazon.com, Inc. sent CyberSource the plaintiff's information for identity verification purposes, but Amazon had received that information at the plaintiff's *express* direction. *Id.* at 1268-69 Here, Plaintiffs sought to prohibit Defendants' from setting and obtaining information from third-party cookies. While Plaintiffs sent certain information to Defendants triggering particular ads, the different information at issue is that which Defendants were able to access through the

[9] *Supra*, sec. IV.A.1.

third-party cookies Defendants impermissibly set. Defendants' factual argument that they accessed no additional information ignores the many contrary pro-Plaintiff inferences and necessitates discovery

Defendants' argument that they were the "intended" recipient of the cookie information fails. Defendants' cookies were never authorized to be set in Plaintiffs' browser-managed files. Any resulting communications related to those cookies are equally unauthorized. Very differently, in *In re DoubleClick* users could have opted out of the cookies. 154 F. Supp. 2d at 504-05. The Plaintiffs here *did* opt out of the cookies, but Defendants secretly disabled that opt out. Likewise, in *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1049-50, plaintiffs had voluntarily downloaded the apps in question. Unlike the *DoubleClick* and *iPhone* plaintiffs, Plaintiffs here voluntarily acted to prevent, not permit, the cookies.

4. Defendants Accessed Information in "Electronic Storage"

Defendants say Plaintiffs' SCA claim fails to allege Defendants accessed any communications in "electronic storage." "Electronic storage" includes "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof…." 18 U.S.C. § 2510(17). Under the SCA Plaintiffs need only plead facts plausibly suggesting that data that Defendants accessed without authorization was temporarily stored pending delivery to an intended recipient. Plaintiffs have pled precisely that. *See* CAC ¶ 218. Plaintiffs allege extensive facts explaining Defendants' scheme, *see* CAC ¶¶ ¶¶ 27-48, 68-78, 153-162, and how the information was stored, *see* CAC ¶¶ 45-46, 153-156, 16. At minimum

these facts "suggest" (*Phillips*, 515 F.3d at 233-35) that Defendants accessed Plaintiffs' data in "electronic storage."[10]

Defendants store their cookies in users' browser-managed files for future use, as, so they are stored in a "facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a). Only Defendants can store the cookies at issue in the browser through which the ECS is provided because Plaintiffs were unaware of the unauthorized placement and storage of these cookies. So, the browser-managed files storing the cookies, in the "facilities" Plaintiffs alleged were accessed without authorization (CAC ¶ 217), are within the SCA's "electronic storage" definition. *See In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1277 (C.D. Cal. 2001) ("Plaintiffs have alleged that Defendant accessed data contained in 'cookies' that it placed in Plaintiffs' computers' electronic storage. The court concludes that this allegation satisfies the liberal requirements of Rule 8(a)(2)."); *see also Cousineau v. Microsoft Corp.*, slip op., No. C11-1438-JCC, at 12 (W.D. Wash. June 22, 2012) (See Ex. 1 attached) ("The language Congress chose, however, does not require only one point of ECS provision."). Defendants' argument that the access must occur while the information is "in the middle of" any transmission (*see* D.Br. 14) is belied by the holdings of other courts in this circuit that have interpreted the Third Circuit's opinion in *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir.2003) not to require that the communication be "in transmission" to be covered by the SCA. *See Markert v. Becker Technical Staffing, Inc.*, Civil Action No. 09–CV–5774, 2010 WL 1856057, at *6 (E.D. Pa. May

[10] Defendants' reliance on *In re DoubleClick* is again misplaced. D. Br. 14. *DoubleClick's* plaintiffs alleged that the data files (cookies) at issue were *permanently* stored on their hard drives, leading the court to conclude, as a matter of law, that the defendants could not have accessed information in temporary "electronic storage." *In re DoubleClick*, 154 F. Supp. 2d at 512. The same is true of *Yunker*, 2013 WL 1282980, at *8-9. Plaintiffs allege that the cookies were temporarily stored by Defendants when Defendants accessed them without permission. Defendants' other cited cases in footnote 8 are distinguishable; none involved cookies set by defendants.

7, 2010) ("we do not believe that it is proper to require that the communication be in the process of transmission in order for it to be covered under the FSCA").[11]

C. COUNT III – PLAINTIFFS HAVE STATED A CFAA CLAIM

3. Plaintiffs Properly Allege the Defendants' CFAA Violation

Defendants argue that Plaintiffs fail sufficiently to allege that Defendants "acted 'without authorization' or 'exceed[ed] authorized access.'" D. Br. 18. Either Defendants did not read the CAC, or they hope the Court has not.

First, the CAC alleges Defendants' business depends on gathering exactly the sort of user data Plaintiffs allege Defendants illicitly took. ¶¶ 25, 26, 156, 157, 161. This fact alone creates many plausible inferences that Defendants knowingly hacked the Safari default setting for business and economic reasons. Safari's default setting prevented the Defendants from getting the "massive amounts of data" needed "to deliver the right ad, to the right person, at the right time." CAC ¶¶ 45, 156. So Defendants engineered a way around the block.

Second, Defendants violated the CFAA's access restrictions. 18 U.S.C. § 1030(a)(2). "Access restrictions" include "*who* may access information, *what* information may be accessed, [and] the *methods* by which information may be accessed." *Craigslist, Inc. v. 3 Taps, Inc.*, No. CV 12–03816 CRB, 2013 WL 1819999, at *4 (N.D. Cal. Apr. 30, 2013) (citing *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir.2012) (en banc), as holding these elements are "more properly considered 'access' restrictions under the CFAA"). Defendants had no express authorization to circumvent Plaintiffs' default browser setting using their hidden ad-embedded codes (*see* CAC ¶¶ 153, 154), triggering invisible iframes and forms (*see* CAC ¶¶ 153, 154), leading to the

[11] Defendants' attempt to argue Plaintiffs' SCA claim is foreclosed by their allegations under the Wiretap Act is a red herring. Plaintiffs are entitled to plead in the alternative. To the extent the communications are in transient storage during transmission (*see United States v. Councilman*, 418 F.3d 67, 82 (1st Cir. 2005) (en banc), both Wiretap and SCA liability apply.

planting of concealed third-party cookies (*see* CAC ¶¶ 153, 154, 156) and permitting Defendants' user information gathering in circumvention of the Safari default setting. *See* CAC ¶¶ 1 ("secret and unconsented-to" use of cookies); 3 (circumvention of "'do not track' privacy settings…to obtain PII without notice or permission"); 4 ("surreptitious circumvention of…privacy controls in order to obtain II without notice or permission"); 160 (Media never said "users consented to, or authorized, Media's secret negation" of Safari default setting); 222 (access to browser-managed files without or in excess of authorization); 224 (access to computers without or in excess of authorization). Defendants' secret cookie-driven data gathering was part and parcel of their very business. *See* CAC ¶¶ 156, 157, 161.

Third, Defendants' multi-step technological legerdemain in defeating the Safari default blocking setting establishes Defendants' violation of the CFAA's access restrictions. *See Craigslist*, 2013 WL 1819999, at *4 (denying motion to dismiss CFAA claim where Defendants' continued use of Craiglist despite, *inter alia*, "the technological measures to block them constitutes unauthorized access under the statute" (citing *Facebook, Inc. v. Power Ventures, Inc. (Facebook II)*, 844 F. Supp. 2d 1025, 1038-39 (N.D. Cal. 2012), as "holding that 'circumvent[ing] technical barriers,' specifically, taking steps to evade the blocking of IP addresses, constitutes 'access[ing] the site 'without permission' and triggers liability under the CFAA.'")).

Defendants argue that Plaintiffs "granted the Moving Defendants permission to access their computers for *some* purpose" (D. Br. 19 (emphasis in original)) by requesting ads. That, Defendants say, constituted permission for their undisclosed implanting of the third-party tracking cookies that Plaintiffs never asked for, never knew about, and believed their default settings blocked. For this absurd proposition Defendants cite *LVRC Holdings, Inc. v. Brekka*,

581 F.3d 1127 (9th Cir. 2009) (D. Br 19). *Brekka* is entirely inapposite, on its summary judgment posture and, even more, on its dispositively different facts.

Brekka involved an employee of a residential treatment center for addicts who, before leaving the company "emailed a number of LVRC documents to his personal email account and his wife's personal email account." *Id.* at 1129-30. Completely different from Defendants' unauthorized and unknown outside-in hack of Plaintiffs' computers and browser files, Mr. Brekka "had authorization to use the LVRC computer" so "he did not access a computer 'without authorization.'" *Id.* at 1135. *Brekka* reflects the "narrow" view of CFAA liability applicable in the Ninth and Fourth Circuits in the "faithless employee" dispute setting that is irrelevant here. *See, e.g. JBCHoldings NY, LLC v. Pakter*, No. 12 Civ. 7555(PAE), 2013 WL 1149061, at *4-*5 (S.D.N.Y. Mar. 20, 2013) (contrasting "broad approach" of the First, Fifth, Seventh, and Eleventh Circuits holding "that the statutory terms 'without authorization' and/or 'exceeds authorized access' are broad enough to reach the situation in which an employee misuses employer information that he or she is otherwise permitted to access" with "narrow approach" of Fourth and Ninth Circuits holding "that the statute does not reach the mere misuse of employer information or violations of company use policies"). *Pakter* shows why Defendants here violated the CFAA: "There is no doubt that the CFAA applies to an 'outside' hacker who remotely enters a computer system without authority to do so." *Id.* at *4.

Defendants' reliance on the "Partial Allowance Setting" (D. Br. 19) to justify their hack is like arguing that a homeowner who lets in a workman thereby authorizes thieves to enter and steal. If "[a] causal chain from the thief to the victim is not broken by a vulnerability that the victim negligently leaves open to the thief" (*Creative Computing v. Getloaded.com, LLC*, 386 F.3d 930 (9th Cir. 2004) (D. Br. 15)), the causal chain surely remains intact when the victim

deliberately uses a cookie-blocking device to prevent such an opening. Anyway, this "some authority means all authority" argument falls on the "exceeds authorized access" CFAA liability prong. 18 U.S.C. § 1030(a)(2).

Defendants argue that Plaintiffs alleged no facts showing Defendants obtained or altered information without authorization. D. Br. 19. But the CAC specifically alleges that Defendants' actions led to unpermitted secret tracking cookies (CAC ¶¶ 153-154, 156, 158, 161), and tracking cookies' central role in obtaining user information. CAC ¶¶ 38-40, 45-46, 78 (using Google as example). Defendants' claim that they only received "cookie values" (D. Br. 20) ignores the CAC's specific facts showing the fundamental information–user associational role cookies play in tracking. *In re DoubleClick*, 154 F. Supp. 2d 497 (D. Br. 20) nowhere supports placement of cookies in deliberate violation of a default blocking setting.

4. Plaintiffs Properly Allege the CFAA's $5,000 Damages Threshold

i. Plaintiffs' Properly Plead their Loss Allegations

Defendants' arguments that Plaintiffs insufficiently plead that Defendants collected Plaintiffs' PII and that such PII has CFAA-required value are based on an inapplicable heightened pleading standard. Plaintiffs have properly given Defendants fair notice of their claim and its grounds, with plausible – admitted – factual allegations raising the reasonable inference that discovery will yield evidence of required elements. *See, e.g., Wilmington Trust,* 2013 WL 1855756, at *6 (quoting *Twombly*, 550 U.S. at 545 ("'interpreting Fed. R. Civ. P. 8(a)") (further citations omitted)). *See also Phillips*, 515 F. 3d at 230 (*Twombly's* plausibility test says complaint survives if it "'simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of' the necessary element" of the claim). *See also Golod v. Bank of America Corp.*, Civil No. 08–746 (NLH)(AMD), 2009 WL 1605309, at *1 (D. Del. June

4, 2009), *aff'd*, 403 Fed. Appx. 699 (3d Cir. 2010) (well settled that pleading suffices if it contains "'a short and plain statement of the claim showing that the pleader is entitled to relief.' Fed. R. Civ. P. 8(a)(2)," citing "liberal federal pleading rules").

ii. Plaintiffs' Properly Plead the CFAA Loss Requirement

Defendants' "insufficient amount" loss arguments depend on a crabbed reading of the CFAA that many courts have rejected. *United Factory Furnishings v. Alterwitz*, No. 2:12-CV-00059, 2012 WL 2138115 (D. Nev. June 13, 2012), involved allegations that former employees secretly accessed the plaintiff's business computer network. The plaintiff claimed it suffered damages "when Defendants accessed sensitive financial information, trade secrets and accounts payable. " *Id.* at *2. Plaintiff also claimed it did "a damage assessment, obtaining a mirror image of computer equipment," and noted "other consequential damages" might be found. *Id.* The defendants argued plaintiff had "not properly alleged specific damages" exceeding the $5,000 CFAA threshold. *Id.* The *Alterwitz* court first stated: "[i]n the CFAA, Congress defined 'loss' broadly to include any reasonable cost, revenue lost, and other consequential damages. 18 U.S.C. §1030(e)(11)." *Id.* Then the court said: "Plaintiff's [sic] avers losses of this type." *Id.* Finding the plaintiff's "alleged losses will aggregate to at least $5,000," the *Alterwitz* court denied defendants' motion to dismiss the CFAA claim. *Id.* The same result is correct here.

CoStar Realty Information, Inc. v. Field, 612 F. Supp. 2d 660 (D. Md. 2009), denied a motion to dismiss plaintiffs' CFAA claim, refusing to limit recoverable losses to those from "interruption of service." *Id.* at 674-75. "Given that Rule 12(b)(6) is a disfavored motion…and accepting the allegations of the complaint as true and in the light most favorable to the plaintiff," the *CoStar* court sustained claims for CFAA losses from unpaid license fees resulting from the

defendant-licensees' permission to non-licensees to use defendants' access to plaintiffs' database. *Id.* at 675.

Denying a motion to dismiss a CFAA claim, *Ervin & Smith Advert. and Public Relations, Inc. v. Ervin*, No. 8:08CV459, 2009 WL 249998 (D. Neb. Feb. 3, 2009), *Ervin* involved claims that two former employees accessed their employer's computers and stole confidential and proprietary information. The *Ervin* court rejected defendants' argument – which Defendants here echo – that the plaintiff had failed to plead satisfaction of the $5,000 loss threshold because "Plaintiff cannot recover any loss of business or revenue Plaintiff incurred as a result of Defendants' actions because of [18 U.S.C.] § 1030(g)'s limitation on recovery to 'economic damages' and the statute's definition of 'loss' allow for recovery of the physical damage done to Plaintiff's computer system only." *Id.* at *8. Like Defendants here, the *Ervin* defendants argued "that any revenue lost outside of restoring computer service or data lost is not recoverable under the Act." *Id.* at *8 n.5. Rejecting that "flawed" interpretation, the *Ervin* court said:

> [S]hould the court adopt the Defendant's reasoning and limit recovery under the CFAA to those instances in which a Plaintiff can demonstrate actual, physical damage to a computer or computer system, this Court's ruling 'would flout Congress's intent' in creating the CFAA. *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 585 (1st Cir. 2001). "As we move into an increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever larger. If we were to restrict the statute as [Defendants] urge, we would flout Congress's intent by effectively permitting the CFAA to languish in the twentieth century, as violators of the Act move into the twenty-first century and beyond." *Id.*

Ervin, 2009 WL 249998, at *9.

Defendants' argument that the CFAA only permits recovery of "'costs'" or losses from "interrupted service" (D. Br. 15) also violates a basic statutory interpretation canon. The CFAA defines "loss" as "any reasonable cost to any victim, including …" followed by a six-item list.

18 U.S.C. § 1030(e)(11). Defendants wrongly read that list as exhaustive, excluding any other losses. But that list is illustrative only, supporting broader CFAA losses. *See In re APA Transport. Corp. Consol. Litig.*, 541 F.3d 233, 241-42 (3d Cir. 2008) ("well-established canon …that when the word 'including' is followed by a list of examples, those examples are generally considered illustrative rather than exhaustive" (citing *Massachusetts v. E.P.A.*, 549 U.S. 497, 127 S. Ct. 1438, 1476 (2007) (Scalia, J., dissenting)).

Defendants' argument that Plaintiffs cannot aggregate losses is simply wrong. Plaintiffs incorporate by reference their argument on this issue in their Opposition to Vibrant Media's Motion to Dismiss, filed this same date, at pp. 15-20.

None of Defendants' loss cases support their arguments. *Creative Computing* 386 F.3d 930 (D. Br. 15), confirms the CFAA cannot be read to "require proof of $5,000 of damage or loss from a single unauthorized access" (*id*. at 934) and "contains no 'single act' requirement." *Id.* at 935. *Creative Computing* rejected the defendant's argument that the CFAA did not permit recovery for "loss of business and business goodwill" (*id.*), finding recoverable "'economic damages'" include losses, like Plaintiffs' (*see, e.g.*, CAC ¶¶ 158, 161), arise "[w]hen an individual's…money or property are impaired in value, or money or property is lost…" *Id.*

Unlike Plaintiffs here, the plaintiffs in *Del Vecchio v. Amazon.com, Inc.*, No. C11–366RSL, 2012 WL 1997697, at *4 (W.D. Wash. June 1, 2012) (D. Br. 16), conceded their information was economically valueless. In *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (D. Br. 16-17), the plaintiffs "*voluntarily downloaded*" the "software that allegedly harmed" their devices. *Id.* at 1066 (emphasis in original). *In re iPhone Application Litig.* (*id.* at 1067) cites *AtPac,Inc. v. Aptitude Solutions, Inc.*, 730 F. Supp. 2d 1174, 1185 (E.D. Cal. 2010), for its narrow view of the CFAA's scope. *AtPac*, however, said the statute's loss definition

confirmed "'Congress's intent to restrict civil actions under subsection (I) to the traditional computer 'hacker' scenario – where the hacker deletes information, infects computers or crashes networks.'" *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1067 (quoting *AtPac*, 730 F. Supp. 2d at 1185).

LaCourt v. Specific Media, Inc., No. SACV 10–1256–GW(JCGx), 2011 WL 1661532, at *2-*4 (C.D. Cal. Apr. 28, 2011) (D. Br. 17), dealt with Article III standing, not our case's statutory standing under the CFAA. Our Plaintiffs have alleged all they need: the invasion of CFAA-protected rights. *See, e.g., Warth v. Seldin*, 422 U.S. 490, 500 (1975) (statutory standing "question...is whether the…statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief.").[12] Factually distinguishable, too, *LaCourt's* plaintiffs barely argued that PII had economic value. *See LaCourt*, 2011 WL 1661532, at *4. Plaintiffs here allege specific dollar values in PII markets. *See* CAC ¶¶ 49-67. *LaCourt's* plaintiffs, unlike ours, alleged not an established past violation, but a tenuous belief that re-visiting certain webites might re-spawn previously deleted cookies. *LaCourt*, 2011 WL 1661532, at *3.

In *In re Zynga Privacy Litig.*, No. C-10-04680 JWW, 2011 WL 7479170, at *3 (N.D. Cal. June 15, 2011) (D. Br. 17 n.10), the plaintiffs offered only two general allegations of loss ("damage or loss by misappropriating and disclosing" PII and that loss aggregated over $5,000). Plaintiffs here allege much more and in great detail. *See* CAC ¶¶ 49-67. The court in *Zynga* said

[12] What Defendants say is a "hotly contested issue" of statutory standing (D. Br. 17 n.11) is an illegitimate effort, rejected by many courts, to graft an additional requirement of injury-in-fact onto the harm that Congress decided was itself, without more, worthy of redress in the federal law at issue. *See, e.g., Alston v. Countrywide Fin. Corp.*, 585 F.3d 753, 763 (3d Cir. 2009); *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010), *cert. dismissed as improvidently granted*, 132 S. Ct. 2536 (June 28, 2012); *Gaos v. Google, Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646, at *3 (N.D. Cal. Mar. 29, 2012).

plaintiffs had not provided any "legal authority" supporting the claim that PII "constitutes a form of money or property." Unlike *Zynga's* plaintiffs (*Zynga*, 2011 WL 7479170, at *3), Plaintiffs here cite cases describing the breadth of recoverable CFAA losses *LaCourt* endorses the theory that *Znyga's* and *LaCourt's* plaintiffs did not develop. *LaCourt*, 2011 WL 1661532, at *4.

In *In re DoubleClick* (D. Br. 17, 17 n.11), among other differences, useful opt-out options existed. 154 F. Supp. 2d at 504-05. Our Plaintiffs did not even know they were being tracked. *In re DoubleClick* and *Bose v. Interclick, Inc.*, No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *6-*7 (S.D.N.Y. Aug. 17, 2011) (D. Br. 17, 17 n.11) erroneously wrote a narrow "single act" exception into the CFAA's loss definition in violation of the law's text and aims. *Cf. In re Toys R Us, Inc. Privacy Litig.*, No. 00-CV-2746, 2001 WL 34517252, at *11 (N.D. Cal. Oct. 9, 2001) (illicit cookie planted on many computers satisfied "same act" requirement); *In re Apple & AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (following *In re Toys R Us*). Neither *In re DoubleClick* nor *Bose* recognized what the *LaCourt* court saw as the inherent value of PII.

V. CONCLUSION

Defendants Media and WPP's Motion to Dismiss should be denied on all Counts.

Dated: May 29, 2013

Respectfully submitted,

KEEFE BARTELS, LLC

/s/ Stephen G. Grygiel
Stephen G. Grygiel (Del Br No. 4944)
John E. Keefe, Jr.
Jennifer L. Harwood
170 Monmouth St.
Red Bank, NJ 07701
Tel: 732-224-9400
sgrygiel@keefbartels.com

Executive Committee Member

STRANGE & CARPENTER

/s/ Brian Russell Strange
Brian Russell Strange
Keith Butler
David Holop
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Tel: 310-207-5055
lacounsel@earthlink.net

Executive Committee Member

BARTIMUS, FRICKLETON, ROBERTSON & GORNY, P.C.

/s/ James P. Frickleton
James P. Frickleton
Mary D. Winter
Stephen M. Gorny
Edward D. Robertston, Jr.
11150 Overbrook Road, Suite 200
Leawood, KS 66211
Tel: 913-266-2300
jimf@bflawfirm.com

Executive Committee Member

FINGER & SLANINA, LLC

/s/ David L. Finger
Charles Slanina (DE Bar ID #2011)
David L. Finger (DE Bar ID #2556)
One Commerce Center
1201 N. Orange St., 7th fl.
Wilmington, DE 19801
(302) 573-2525
dfinger@delawgroup.com

Liaison Counsel

EICHEN, CRUTCHLOW, ZASLOW & MCELROY LLP

/s/ Barry Eichen
Barry R. Eichen
40 Ethel Road
Edison, NJ 08817
Tel: 732-777-0100
beichen@njadvocates.com

Plaintiffs' Steering Committee Member

SEEGER WEISS LLP

/s/ Jonathan Shub
Jonathan Shub
1515 Market Street, Suite 1380
Philadelphia, PA 19102
Tel: 215-564-2300
jshub@seegerweiss.com

Counsel for Plaintiff Lynne Krause and Plaintiffs' Steering Committee Member

MURPHY P.A.

/s/ William H. Murphy, Jr.
William H. Murphy, Jr.
One South Street, Suite 2300
Baltimore, MD 21202
Tel: 410-539-6500
billy.murphy@murphypa.com

Plaintiffs' Steering Committee Member

BARNES & ASSOCIATES

/s/ Jay Barnes
Jay Barnes
219 East Dunklin Street
Jefferson City, MO 65101
Tel: 573-634-8884
Jaybarnes5@gmail.com

Plaintiffs' Steering Committee Member

BRYANT LAW CENTER, PSC

/s/ Mark Bryant
Mark Bryant
601 Washington Street
P.O. Box 1876
Paducah, KY 42002-1876
Tel: 270-442-1422
mark.bryant@bryantpsc.com

Counsel for Plaintiff William G. Gourley and Plaintiffs' Steering Committee Member